

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PÄTENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
13. Januar 2005 (13.01.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/004433 A1

(51) Internationale Patentklassifikation⁷: H04L 29/06,
29/12, 12/28, 12/56

(21) Internationales Aktenzeichen: PCT/EP2004/051153

(22) Internationales Anmeldedatum:
17. Juni 2004 (17.06.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 27 610.6 18. Juni 2003 (18.06.2003) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): SIEMENS AKTIENGESELLSCHAFT [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): CUELLAR, Jorge
[DE/DE]; Höllriegelskreuther Weg 14, 82065 Baierbrunn
(DE). TSCHOFENIG, Hannes [AT/DE]; Atterseestr. 15,
81241 München (DE).

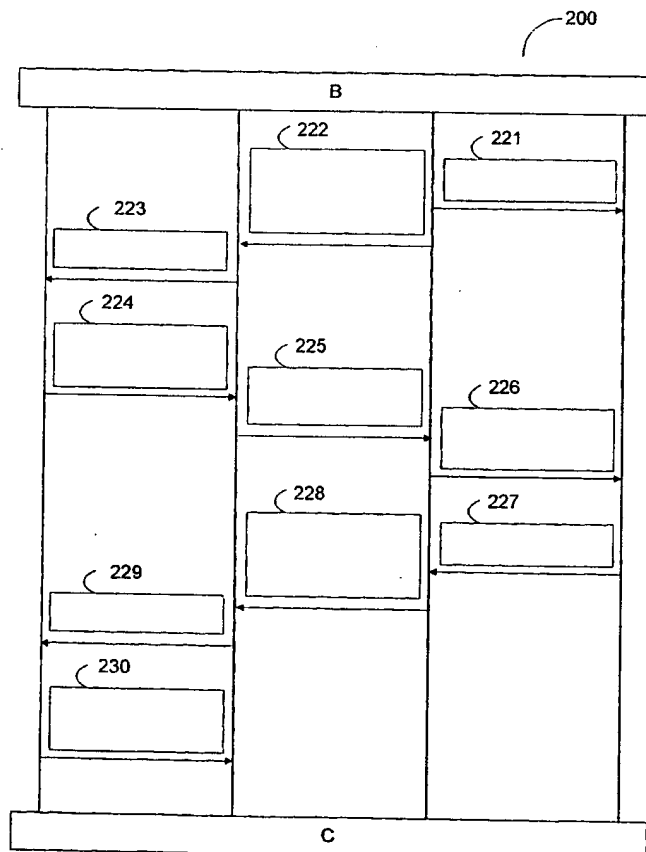
(74) Gemeinsamer Vertreter: SIEMENS AKTIENGE-
SELLSCHAFT; Postfach 22 16 34, 80506 München
(DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR FORMING AND ENCRYPTING AN ENCRYPTED MESSAGE CONTAINING COM-
MUNICATION CONFIGURATION DATA

(54) Bezeichnung: VERFAHREN UND EINRICHTUNG ZUM BILDEN UND ENTSCHLÜSSELN EINER VERSCHLÜSSEL-
TEN NACHRICHT MIT KOMMUNIKATIONS-KONFIGURATIONSDATEN



(57) Abstract: A cryptographic key pair is formed
(226) using an Internet-based authentication method,
in order to transmit (230) communication configuration
data from a first communication unit to a second
communication unit in a secure cryptographic manner.

(57) Zusammenfassung: Mittels eines Inter-
net-basierten Authentifikationsverfahrens wird
ein kryptographisches Schlüsselpaar gebildet
(226), welches verwendet wird, um Kommu-
nikations-Konfigurationsdaten von einer ersten
Kommunikationseinheit zu einer zweiten Kommu-
nikationseinheit kryptographisch gesichert zu übertragen
(230).

BEST AVAILABLE COPY

WO 2005/004433 A1



MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht

- (84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT,

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

BEST AVAILABLE COPY